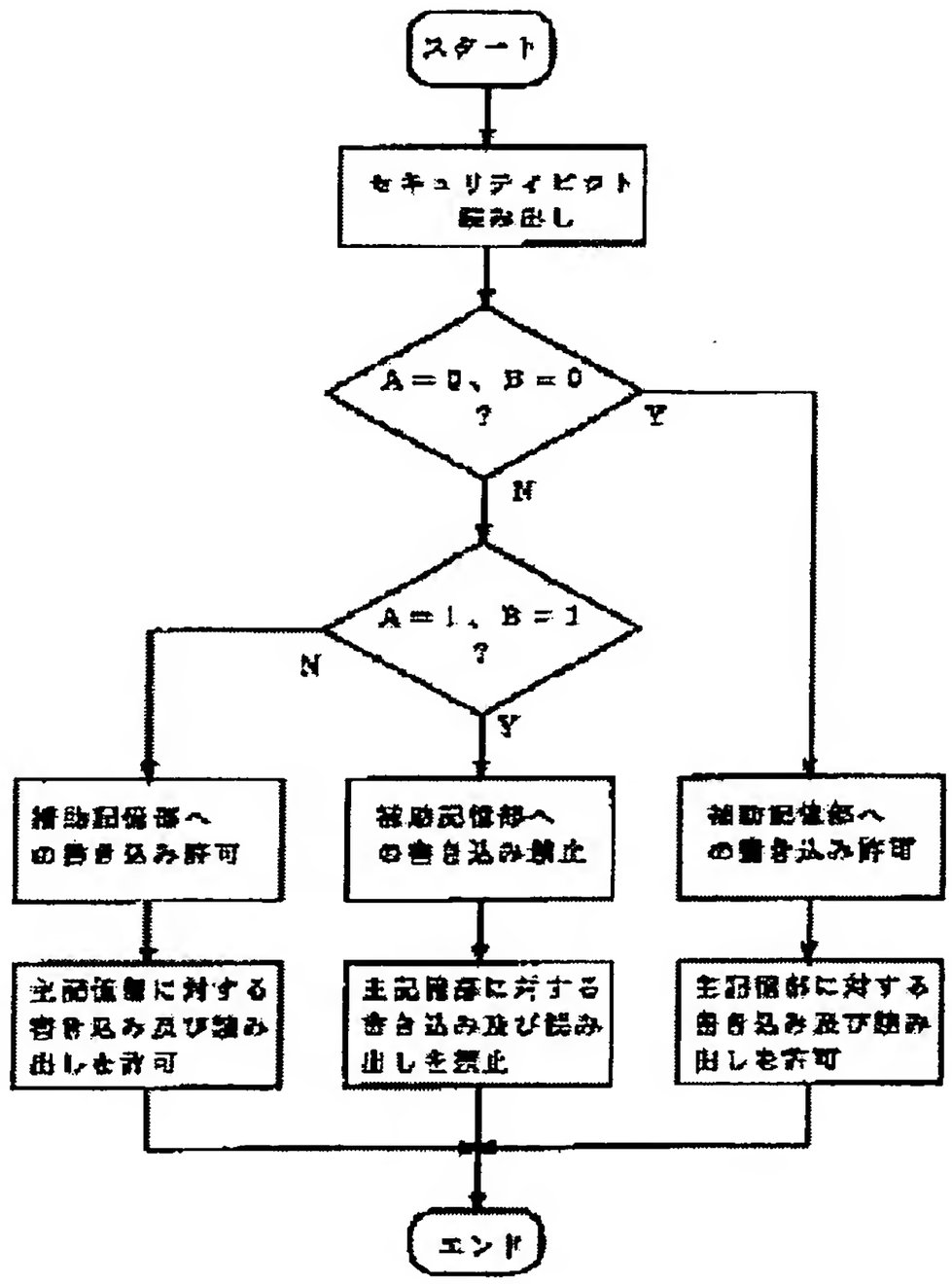
DATA PROCESSOR

Patent number: JP10228422
Publication date: 1998-08-25
Inventor: USAMI MASA; KONDO HIDEKI; KAMIO SHIGEKI
Applicant: MOTOROLA JAPAN
Classification:
- international: ***G06F12/14;*** **G06F12/14;** (IPC1-7): G06F12/14; G06F15/78
- european: G06F12/14C1A
Application number: JP19970047091 19970214
Priority number(s): JP19970047091 19970214

Also published as:
US6076149 (A

Abstract of **JP10228422**

PROBLEM TO BE SOLVED: To attain storage protection and secrecy holding for a program or the like with respect to a data processor provided with a main storage part consisting of a non-volatile memory and a CPU. SOLUTION: An auxiliary storage part for storing security bit data is included in an erasable programmable read-only memory(EEPROM) constituting a main storage part e.g. When the read result of the CPU at the time of allowing a current to flow between the drain and source of a transistor(TR) in the EEPROM is set up to '0' and a read result when the current is not allowed to flow is set up to '1', security bit data read out from two TRs A, B are A=1, B=1 and an access to the main storage part and writing in the auxiliary storage part are set up so as to be inhibited. When A=0 and B=0, security is applied but writing in the auxiliary storage part is permitted, and when A=1(0) and B=0(1), security is set up so as to be released.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－228422

(43)公開日　平成10年(1998)８月25日

(51)Int.Cl.[6]	識別記号	ＦＩ		
G06F 12/14	320	G06F 12/14	320	A
15/78	510	15/78	510	A

審査請求　未請求　請求項の数３　ＦＤ　（全８頁）

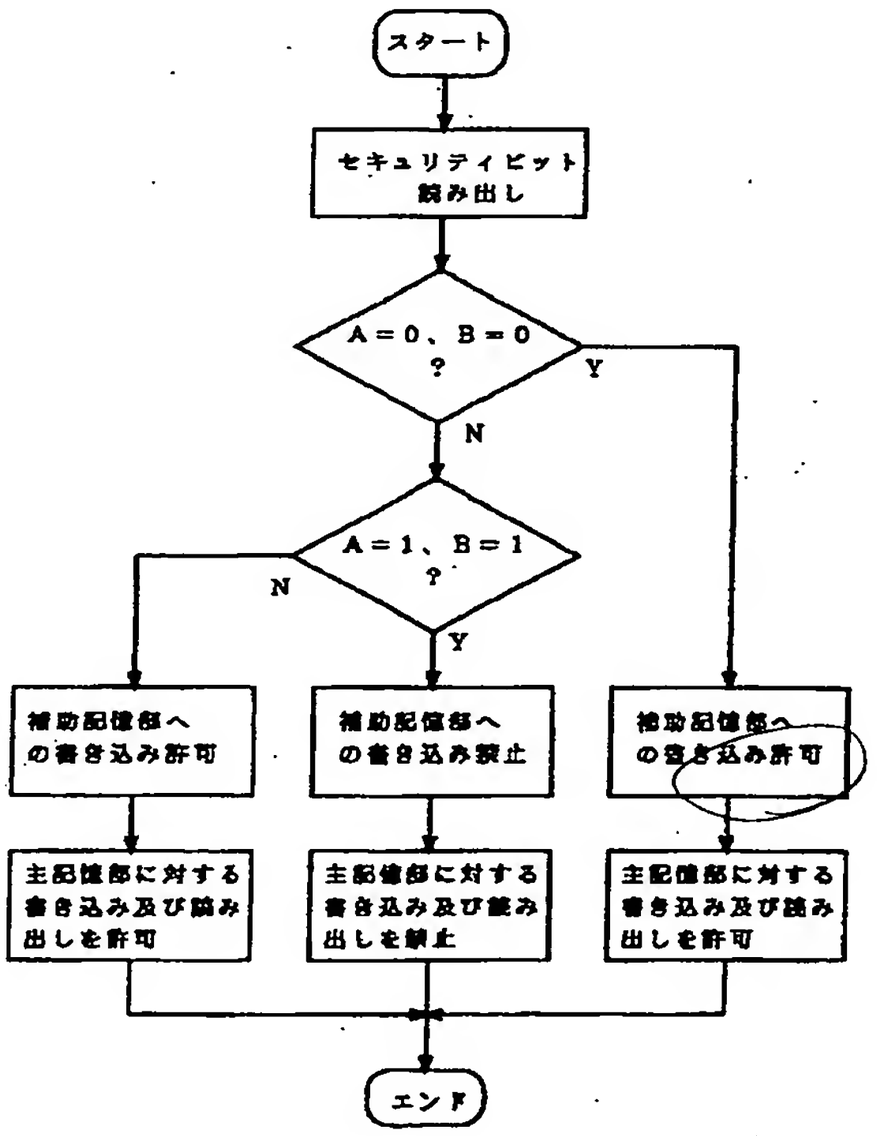
(21)出願番号　特願平9－47091

(22)出願日　平成９年(1997)２月14日

(71)出願人　000230308
日本モトローラ株式会社
東京都港区南麻布３丁目20番１号
(72)発明者　宇佐美　雅
東京都港区南麻布３丁目20番１号　日本モトローラ株式会社内
(72)発明者　近藤　秀樹
東京都港区南麻布３丁目20番１号　日本モトローラ株式会社内
(72)発明者　神尾　茂樹
東京都港区南麻布３丁目20番１号　日本モトローラ株式会社内
(74)代理人　弁理士　井上　俊夫

(54)【発明の名称】データ処理装置

(57)【要約】
【課題】　不揮発性メモリよりなる主記憶部とＣＰＵとを備えたデータ処理装置において、プログラム等の記憶保護及び機密保持を図ること。
【解決手段】　セキュリティビットデータを格納する補助記憶部を、例えば主記憶部を構成するＥＰＲＯＭの中に設ける。ＥＰＲＯＭのトランジスタのドレイン、ソース間に電流が流れたときのＣＰＵの読み出し結果を「０」、前記電流が流れないときの読み出し結果を「１」とすると、２個のトランジスタＡ、Ｂから読み出したセキュリティビットデータがＡ＝１、Ｂ＝１で、主記憶部に対するアクセス及び補助記憶部に対する書き込みを禁止するように設定する。またＡ＝０、Ｂ＝０でもセキュリティがかかるが補助記憶部に対する書き込みは許可し、更にＡ＝１（０）、Ｂ＝０（１）でセキュリティが解除されるように設定する。



【特許請求の範囲】

【請求項１】　データを記憶する不揮発性メモリよりなる主記憶部と、

この主記憶部に対する読み出し及び書き込みを制限するためのビットデータを記憶するプログラマブルＲＯＭよりなる補助記憶部と、

前記主記憶部及び補助記憶部に対して読み出し及び書き込みを行うための処理部と、を備え、

前記ビットデータは、プログラマブルＲＯＭのメモリセルであって、ゲートに電圧印加信号線が接続された２個以上のトランジスタのドレイン、ソース間が導通するときのゲート電圧の各しきい値の高低に対応し、

前記処理部は、前記トランジスタのドレイン、ソース間に電流が流れたときの読み出しビットデータを「０」、前記電流が流れなかったときの読み出しビットデータを「１」と定義すると、前記補助記憶部から読み出したビットデータの組み合わせに基づいて以下のａ～ｃの処理を行うように構成されていることを特徴とするデータ処理装置。

ａ．各ビットデータがすべて「０」であれば、前記補助記憶部に対する書き込みを許可すると共に前記主記憶部に対する外部からの書き込み及び読み出しを禁止する。

ｂ．各ビットデータがすべて「１」であれば、前記補助記憶部に対する書き込みを禁止すると共に前記主記憶部に対する外部からの書き込み及び読み出しを禁止する。

ｃ．「１」、「０」が混在しているビットデータの組み合わせの中で少なくとも一つの組み合わせに対して、当該補助記憶部に対する書き込みを許可すると共に前記主記憶部に対する外部からの書き込み及び読み出しを許可する。

【請求項２】　主記憶部は、補助記憶部と同種のプログラマブルＲＯＭよりなり、補助記憶部の記憶内容を消去すると主記憶部の記憶内容も同時に消去されるように構成されていることを特徴とする請求項１記載のデータ処理装置。

【請求項３】　補助記憶部は、主記憶部をなすメモリアレイの中に組み込まれていることを特徴とする請求項２記載のデータ処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、記憶部や処理部を備えたデータ記憶装置に係り、例えば１チップのコントローラユニットに含まれるメモリに対して記憶保護及び機密保持を図ることができ、あるいは出荷時に行う機能テストプログラムに対してユーザの起動を防止することができる装置に関する。

【０００２】

【従来の技術】一般にＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）及びＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）を搭載した１チップのマイコンにおいて、ＲＯＭの中に格納されているデータ、例えばゲームソフトや管理情報などを第三者に読み出されないようにすること、及びＲＯＭの中のデータを外部からハッカーによって書き換えられないようにすることが必要になる。

【０００３】プログラムを開発する段階では、プログラムの修正などのために外部のＲＯＭにチップを接続して、チップの中のＲＯＭからデータを読み出すため、アドレスバス及びデータバスの信号について外部との間で授受ができるように、入出力ポートが動作可の状態になっていなければならない。これに対してプログラムの開発後は、入出力ポートにおけるデータバス及びアドレスバスの外部との接続を禁止し、セキュリティをセットすることが必要である。ここでいうセキュリティをセットするとは、ＲＯＭの記憶保護（外部からのデータの書き換えに対する保護）及び機密保持（外部からの読み出しに対する保護）を図ることを意味する。

【０００４】このため従来からレジスタにセキュリティビットを立て、このビットが立っているときは入出力ポートの動作を禁止する一方、セキュリティを解除するときにはパスワードを入力する、あるいは外部端子に所定の論理信号の組み合わせを入力するといった手法が知られている。しかしながらこの方法ではパスワードや信号の組み合わせが第三者に知られてしまえば意味がなくなるし、パスワード等の組み合わせを追いかければ見つかってしまうおそれもある。

【０００５】そこで本発明者はセキュリティビットデータを書き込む記憶部（これを補助記憶部と呼ぶことにする）としてＥＰＲＯＭ（Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍａｂｌｅ　ＲＯＭ）に着目した。例えばＥＰＲＯＭの１個のフローティングゲート型メモリセルであるトランジスタを用いて１ビットのセキュリティビットデータを書き込むとすると、図５に示すようにトランジスタ１０のゲートとソースに夫々電源の一端（Ｖｄｄ）及び他端（Ｖｓｓ）を接続するようにし、このトランジスタ１０のゲートに高電圧を印加してフローティングゲートに電荷を蓄積させる。このときの読み出し結果を「１」と定義すると、第三者がＣＰＵを作動させても、ＣＰＵが先ずセキュリティビットデータを読みにいき、その結果が「１」であるから、入出力ポートにおけるデータバス及びアドレスバスの外部との接続が禁止される。

【０００６】図６はトランジスタ１０のゲート電圧とドレイン電流との関係を示したものであり、紫外線の照射によりフローティングゲートの電荷を消失させた後においてはゲート電圧が低くても電流が流れるが、プログラム時はつまり高電圧をゲートに印加した後は、ゲート電圧を高くしなければ電流が流れない。そして図６において電気的には左から右にいくが、右から左には行かない。即ちトランジスタのしきい値が一旦高くなると、しきい値はそれ以上下がらなくなる。従ってＥＰＲＯＭを

用いてセキュリティを一旦セットすれば、通常これを解除することができない。

【０００７】しかしながらプログラム時にゲートに印加した高電圧よりも更に高い電圧（図６中Ｖ１＋α）をゲートに印加すればトランジスタ１０に電流が流れ、セキュリティビットデータの読み出し結果が見かけ上「０」になってしまうのでセキュリティが解除された状態となってしまう。

【０００８】このため図７に示すようにＥＰＲＯＭのメモリセルであるトランジスタを２個用いて２ビットのセキュリティビットデータとすることを検討している。ここでメモリセルからの読み出し結果については図８に示すように定義するものとする。即ちＥＰＲＯＭに紫外線を照射してメモリセルのフローティングゲートに負電荷の蓄積がない状態でＣＰＵが当該メモリセルから読み出した結果を「０」とし、メモリセルにプログラムを行って（ゲートに高電圧を印加して）フローティングゲートに負電荷が蓄積された状態でＣＰＵが読み出した結果を「１」として説明していく。

【０００９】図７に示す２個のトランジスタを夫々Ａ、Ｂとすると、これらトランジスタＡ、Ｂから読み出したセキュリティビットデータとセキュリティの状態との関係については図９に示すように設定する。この場合Ａ＝１、Ｂ＝１（トランジスタＡ（Ｂ）から読み出したビットデータが１であるという意味である）のときにセキュリティがセットされるとすると、ユーザはＡ＝０（１）、Ｂ＝１（０）のときに主記憶部であるＲＯＭに所定のプログラムやデータを書き込み、その後Ａ＝１、Ｂ＝１とする。このようにすれば既に図６に基づいて述べたようにＥＰＲＯＭは電気的には「１」→「０」にはならないので、第三者はＡ＝０（１）、Ｂ＝１（０）とすることができない。

【００１０】ここでプログラムなどのデータを記憶する主記憶部としてＥＰＲＯＭよりなるメモリアレイを用い、このメモリアレイの中にセキュリティビットデータを入れ込んでおけば、紫外線の照射によりＡ＝０、Ｂ＝０としてセキュリティを解除したとしても、プログラムそのものも消失してしまい、これを読み出すことができなくなる。

【００１１】しかしながら上述のように高い電圧（Ｖ１＋α）をゲートに印加することにより、主記憶部の記憶内容を消去することなくＡ＝０、Ｂ＝０としてＣＰＵに認識させることができる。このためＡ＝０、Ｂ＝０の場合もセキュリティのセット状態としておかなければならないが、チップメーカが紫外線をＥＰＲＯＭに照射してチップをユーザに出荷するときにおいてもＡ＝０、Ｂ＝０であるから、セキュリティがセットされた状態になってしまう。

【００１２】従って正規のユーザがチップを受け入れた後、このセキュリティをどのようにして解除するかが問題となる。セキュリティを解除する手法としては、パスワードの入力、チップの特定のピンに外部から所定の論理信号や所定の電圧を与える、などが考えられるが、ＥＰＲＯＭにセキュリティビットデータを書き込むというそもそもの発想は、パスワードの入力やピンに信号を入力する手法では既述のような問題があるのでこれを回避しようという点にあったので、ＥＰＲＯＭを用いる意味が薄れてしまう。

【００１３】本発明はこうした背景の下になされたものであり、不揮発性メモリよりなる記憶部に格納されているデータ（プログラムや管理情報などの記憶内容）に対して記憶保護及び機密保持効果の高いデータ処理装置を提供することにある。

【００１４】

【課題を解決するための手段】本発明は、データを記憶する不揮発性メモリよりなる主記憶部と、この主記憶部に対する読み出し及び書き込みを制限するためのビットデータを記憶するプログラマブルＲＯＭよりなる補助記憶部と、前記主記憶部及び補助記憶部に対して読み出し及び書き込みを行うための処理部と、を備え、前記ビットデータは、プログラマブルＲＯＭのメモリセルであって、ゲートに電圧印加信号線が接続された２個以上のトランジスタのドレイン、ソース間が導通するときのゲート電圧の各しきい値の高低に対応し、前記処理部は、前記トランジスタのドレイン、ソース間に電流が流れたときの読み出しビットデータを「０」、前記電流が流れなかったときの読み出しビットデータを「１」と定義すると、前記補助記憶部から読み出したビットデータの組み合わせに基づいて以下のａ～ｃの処理を行うように構成されていることを特徴とするデータ処理装置。

【００１５】ａ．各ビットデータがすべて「０」であれば、前記補助記憶部に対する書き込みを許可すると共に前記主記憶部に対する外部からの書き込み及び読み出しを禁止する。

【００１６】ｂ．各ビットデータがすべて「１」であれば、前記補助記憶部に対する書き込みを禁止すると共に前記主記憶部に対する外部からの書き込み及び読み出しを禁止する。

【００１７】ｃ．「１」、「０」が混在しているビットデータの組み合わせの中で少なくとも一つの組み合わせに対して、当該補助記憶部に対する書き込みを許可すると共に前記主記憶部に対する外部からの書き込み及び読み出しを許可する。

【００１８】プログラマブルＲＯＭとしては、ＥＰＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリなどを挙げることができる。主記憶部に対する外部からの書き込み及び読み出しを禁止するとは、例えば１チップマイコンであれば、チップの外から主記憶部に対してアクセスができないという意味である。

【００１９】前記ｃ項の意味は、読み出したビットデー

5

タが、「１」、「０」が混在する組み合わせでありさえすれば、どの組み合わせであっても、補助記憶部に対する書き込みを許可すると共に前記主記憶部に対する外部からの書き込み及び読み出しを許可するようにしてもよいし（つまりセキュリティが解除されるようにしてもよいし）、ある組み合わせについてはセキュリティが解除されるが、他の組み合わせについてはセキュリティがセットされるようにしてもよい。

【００２０】そして例えばユーザが１チップマイコン内へのプログラムの格納を終了した後のセキュリティのセットについては、補助記憶部内のビットデータが全て「１」の組み合わせとしてもよいし、「１」、「０」が混在する組み合わせであっても、セキュリティがかかるものであればその組み合わせとしてもよい。ただし後者の場合には、セキュリティをセットしたビットデータからセキュリティを解除したビットデータへ移行するときに「１」から「０」へ移行するビットを含むようにすることが必要である。プログラマブルＲＯＭの特性から各メモリセルは個別には「１」から「０」へ移行せず、この点に着目してセキュリティを解除するビットデータを第三者が作り出せないようにしているからである。上記のように構成することにより第三者がセキュリティを解除することが困難になる。

【００２１】また主記憶部は補助記憶部と同種のプログラマブルＲＯＭよりなり、補助記憶部の記憶内容を消去すると主記憶部の記憶内容も同時に消去されるように構成してもよい。この場合の例を挙げれば、主記憶部をＥＰＲＯＭで構成し、そのメモリアレイの中に補助記憶部が組み込まれる。

【００２２】

【発明の実施の形態】本発明のデータ処理装置を、１チップのマイクロコントローラユニット（ＭＣＵ）に適用した実施の形態について説明する。この実施の形態は、「発明が解決しようとする課題」の項で述べた、２ビットのセキュリティビットデータによりセキュリティをセットする手法において更なる検討を加えたものであり、紫外線をＥＰＲＯＭに照射してセキュリティビットデータの組み合わせが「０」、「０」のときには、補助記憶部（セキュリティ回路）に対しては書き込みができるようにしたものである。

【００２３】図１はデータ処理装置の主要な構成を示すブロック図であり、鎖線内がＭＣＵチップ２の内部を示している。このチップ２には、外部との間で信号の授受を行うための入出力ポートを備えており、この入出力ポート３はデータバス４１、及びアドレスバス４２に接続されている。チップ２の中に設けられた構成要素について述べると、ポート制御部３１は入出力ポート３をコントロールするためのもので、外部からのアクセスを禁止するときには、データバス４１及びアドレスバス４２に対する外部からの接続を禁止する。ただしこの場合入出

6

力ポート３を通じて図示しない信号線を通じてコントロール信号などは通過できる。

【００２４】ＣＰＵ３２は、主記憶部５１に対しアクセスを行って演算を行ったり、補助記憶部５２のビットデータを読み出してポート制御部３１にその結果を送ったりするなど、チップ内のおもだった処理を行う。モード制御部３３は外部入力例えばキーボードの入力やピンへの信号の組み合わせなどに基づいて、補助記憶部５２内のビットデータを書き換えて、セキュリティのセットモードまたはセキュリティの解除モードの一方を選択する。なおポート制御部３１及びモード制御部３３は、説明の便宜上ブロックとして別個に記載してあるが、この実施の形態では、実際にはＣＰＵ３２の機能の中に含まれている。

【００２５】主記憶部５１は例えばゲームソフトや管理情報などのデータを格納するためのものであり、例えばＥＰＲＯＭにより構成される。補助記憶部５２はセキュリティビットデータを格納するためのものであり、例えばＥＰＲＯＭにより構成される。この補助記憶部５２は、説明の便宜上主記憶部５１と別個に記載してあるが、この実施の形態では実際には、主記憶部５１を構成するメモリアレイの中に組み込まれており、チップの窓から紫外線を照射すると主記憶部５１の記憶内容と共に同時に消去されるようになっている。

【００２６】ただし本発明では補助記憶部５２は主記憶部５１のメモリアレイとは別個に設けられてもよい。図中５３は書き込み／読み出し（Ｒ／Ｗ）信号線であり、主記憶部５１及び補助記憶部５２の書き込み／読み出しを制御するための信号をＣＰＵ３２から出力するためのものである。　前記補助記憶部５２は、ＥＰＲＯＭの一部をなしており、図２に示すように構成される。これは通常のＥＰＲＯＭのメモリアレイの一部であり、特別な構成を備えているわけではない。Ａ、Ｂは各々メモリセルをなすトランジスタであり、ゲートが共通の電圧信号線６１に接続されている。この電圧信号線６１は、バッファ６２を介して行デコーダ６３に接続されている。バッファ６２は、書き込み時には例えば１０～１５Ｖの電圧を電圧信号線６１に印加し、読み出し時には例えば５Ｖの電圧を電圧信号線６１に印加するものである。

【００２７】トランジスタＡ、Ｂのドレインは列デコーダ６４及びセンスアンプ６５を介してデータバス４１に接続されている。Ｒ／Ｗ制御部６６は、前記Ｒ／Ｗ信号線５３からのＲ／Ｗ信号に基づいてセンスアンプ６５に組み込まれているスイッチ部を制御し、データバス４１からの信号がトランジスタＡ、Ｂに書き込まれ、またトランジスタＡ、Ｂのデータ（トランジスタの動作状態）がデータバス４１に読み出されるようになっている。トランジスタＡ、Ｂはセキュリティビットデータを記憶するものであり、読み出し用の電圧がゲートに印加されたときにドレイン、ソース間に電流が流れたときにはデー

タバス４１の対応する信号線に論理「０」が現われ、ドレイン、ソース間に電流が流れないときにはデータバス４１の対応する信号線に論理「１」が現われるようになっている。

【００２８】ここで前記ＣＰＵ３２におけるセキュリティに関する機能について説明する。ＣＰＵ３２が補助記憶部５２のトランジスタＡ、Ｂから読み出した結果が「０」、「０」であるときＡ＝０、Ｂ＝０として記述するものとすると、Ａ＝０、Ｂ＝０のときには主記憶部５１に対しては、外部からの書き込み及び読み出しを禁止すると共に、補助記憶部５２に対しては外部から書き込みができるようにプログラムを組んでいる。具体的には入出力ポート３においてデータバス４１及びアドレスバス４２の外部との接続を禁止しているが、補助記憶部５２だけに対しては図示しない信号線により外部からモード制御部３３を介してアクセスすることができ、前記Ｒ／Ｗ制御部６６に書き込み信号が入力されるように構成される。

【００２９】またＡ＝１、Ｂ＝１のときには主記憶部５１に対する外部からの書き込み及び読み出しを禁止すると共に、前記Ｒ／Ｗ制御部６６に書き込み信号が与えられないようにして補助記憶部５２に対する書き込みをも禁止している。更に（Ａ＝１、Ｂ＝０）あるいは（Ａ＝０、Ｂ＝１）のときには上述の入出力ポート３の制限を解除して外部から主記憶部５１に対する読み出し及び書き込みを許可し、補助記憶部５２に対しても書き込みを許可している。

【００３０】従って外部からＣＰＵ３２を作動させると、そのフローは例えば図３に示すように表わされる。このフローは、ＣＰＵ３２の機能を概念的に表わしたものであり、先ず補助記憶部５２からセキュリティビットデータが読み出されて解読される。例えばＡ＝０、Ｂ＝０であれば補助記憶部５２への書き込みを行うことができ、その書き込みを行わなければ主記憶部５１に対しては外部からアクセスできない。この場合補助記憶部５２に対してＡ＝１、Ｂ＝０を書き込めば、Ａ＝１、Ｂ＝０のフローへ進むのでセキュリティが解除されることになる。

【００３１】例えば１チップのＭＣＵを半導体ウエハから切り出し、これをユーザに出荷し、ユーザがこのＭＣＵを機器に組み込んで市場に出す場合の一連の流れを図４に示す。先ずメーカ側ではウエハから切り出したＭＣＵチップをパッケージ化し、ＥＰＲＯＭに紫外線を照射する。主記憶部５１及び補助記憶部５２はＥＰＲＯＭであるメモリアレイの中に組み込まれているので記憶内容は全て「０」（トランジスタのゲート電圧のしきい値が低い状態）である。このままではＡ＝０、Ｂ＝０でセキュリティがセットされているが、補助記憶部５２に対しては書き込みが可能であるから、Ａ＝１、Ｂ＝０としてセキュリティを解除し、ＭＣＵチップをユーザに出荷する。

【００３２】ユーザはＭＣＵチップの主記憶部５１に所定のプログラムを書き込み、その後Ａ＝１、Ｂ＝１としてセキュリティをセットする。ここで第三者がこのＭＣＵチップを手に入れ、主記憶部５１のプログラムを読み出すためにセキュリティを解除しようとして、補助記憶部５２のトランジスタＡ、Ｂのゲートに高電圧を印加し、セキュリティビットデータを見かけ上Ａ＝０、Ｂ＝０にしたとする。このとき外部から補助記憶部５２に対して書き込みができるため、その書き込みを行おうとするが、トランジスタＡ、Ｂのゲートには既に高電圧が印加されてフローティングゲートに負電荷が蓄積されているので、ＡもＢも「１」にしかなり得ず、Ａ＝１、Ｂ＝１となる。これはセキュリティがセットされている状態なので、結局セキュリティを解除することができない。

【００３３】そこで第三者がＥＰＲＯＭに紫外線を照射してＡ＝０、Ｂ＝０とすれば、Ａ＝１、Ｂ＝０（あるいはＡ＝０、Ｂ＝１）と書き込むことができるのでセキュリティが解除されるが、このとき主記憶部５１の記憶内容も消失するため第三者にとっては結局初期の目的が達成できない。従って上述の実施の形態によれば記憶内容の保護及び機密保護を図ることができる。またチップの製造時においてもパスワード等を用いなくてもセキュリティをセットすることができ、このようにいわば「秘密のカギ」を介在させなくてよいので、この面からも大きなセキュリティ効果が得られる。

【００３４】上述の実施の形態において、セキュリティが解除されるセキュリティビットデータをＡ＝０、Ｂ＝１のみとし、Ａ＝１、Ｂ＝０の場合にはセキュリティがセットされるようにしてもよい。この場合ユーザがＡ＝１、Ｂ＝１とする代りにＡ＝１、Ｂ＝０としてセキュリティをセットしてもよい。Ａ＝１、Ｂ＝０としてセキュリティをセットすれば、第三者がトランジスタＡ、Ｂのゲートに高電圧を印加して見かけ上Ａ＝０、Ｂ＝０とした後もＡ＝０、Ｂ＝１の組み合わせは作り出せないので同様の効果がある。

【００３５】また本発明では３個以上のセキュリティビットデータを用いてもよい。補助記憶部５２の中に例えばトランジスタＡ、Ｂに加えてトランジスタＣが存在するとすれば、Ａ＝０、Ｂ＝０、Ｃ＝０のときにはセキュリティはセットされるが、補助記憶部５２への書き込みは許可されるようにし、Ａ＝１、Ｂ＝１、Ｃ＝１のときには、補助記憶部５２への書き込みも禁止されるようにする。そしてその他の組み合わせ、つまり「０」、「１」が混在する組み合わせについては、その中の少なくとも一つの組み合わせについてセキュリティが解除されるようにしておけば同様の効果が得られる。

【００３６】ただし補助記憶部５２へセットするセキュリティビットデータがＡ＝１、Ｂ＝１、Ｃ＝１であれば、「０」、「１」が混在する組み合わせを作り出すこ

9

とはできないが、補助記憶部５２へセットするセキュリティビットデータが「０」、「１」の混在する組み合わせであれば、セキュリティを解除するセキュリティビットデータは、電気的に移行しない組み合わせを含むことが必要である。例えばＡ＝０、Ｂ＝０、Ｃ＝１としてセキュリティをセットしたとすると、Ａ＝０、Ｂ＝１、Ｃ＝１の組み合わせは、Ｂを０→１に移行させれば（この移行は電気的に可能）作り出すことができるので、セキュリティを解除するビットデータとしては使用できないが、Ａ＝１、Ｂ＝１、Ｃ＝０の組み合わせであれば、Ｃを「１」→「０」に移行させなければならないので（この移行は電気的には不可能）作り出すことができず、従ってセキュリティを解除するビットデータとして使用できる。なおセキュリティビットデータを多くすれば外部からノイズを入れてセキュリティを解除するビットデータを偶然に作り出すおそれが少なくなる。

【００３７】以上において、本発明はゲームソフトなどの第三者による読み出しやデータ破壊を防止するための使用に限らず、メーカが出荷時に行う出荷テスト（機能テスト）のためのテストプログラムをユーザが起動できないようにするために用いてもよい。即ち出荷時のテストプログラムをユーザが起動させるとそのチップが使用できなくなる場合があり、チップ保護の目的からユーザがこのテストプログラムに対してアクセスできないようにすることが望ましい。そこで上述実施の形態に対応させると、メーカ側で補助記憶部５２内のビットデータをＡ＝０（１）、Ｂ＝１（０）に設定し、主記憶部内のテストプログラムを起動して所定の出荷テストを行った後、Ａ＝１、Ｂ＝１としてユーザに出荷すれば、ユーザが誤ってテストプログラムを起動するおそれがなくなる。

【００３８】

【発明の効果】以上のように本発明によれば、主記憶部に格納されているデータに対して高い記憶保護及び機密保持効果が得られる。

【図面の簡単な説明】

【図１】本発明の実施の形態であるデータ処理装置の全体構成を示す構成図である。

【図２】本発明の実施の形態に用いられる補助記憶部を示す回路図である。

【図３】本発明の実施の形態の処理の流れを示すフローチャートである。

【図４】データ処理装置の製造時から、第三者がプログラムの読み出しを試みるまでのセキュリティビットデータと装置の状態との対応関係を示す説明図である。

【図５】セキュリティをセットするための比較例を示す回路図である。

【図６】ＥＰＲＯＭ内のトランジスタの電流、電圧特性を示す特性図である。

【図７】セキュリティをセットするための他の比較例を示す回路図である。

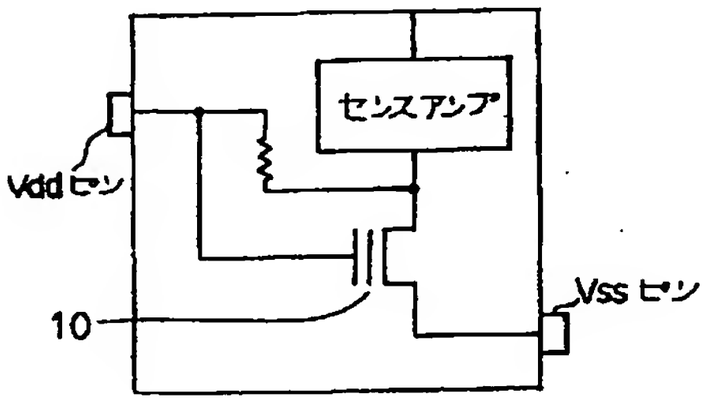
【図８】補助記憶部からの読み出し結果と処理状態との対応を定義付けるための説明図である。

【図９】２ビットのセキュリティビットデータを用いた場合の読み出し結果とセキュリティの状態との対応を示す説明図である。

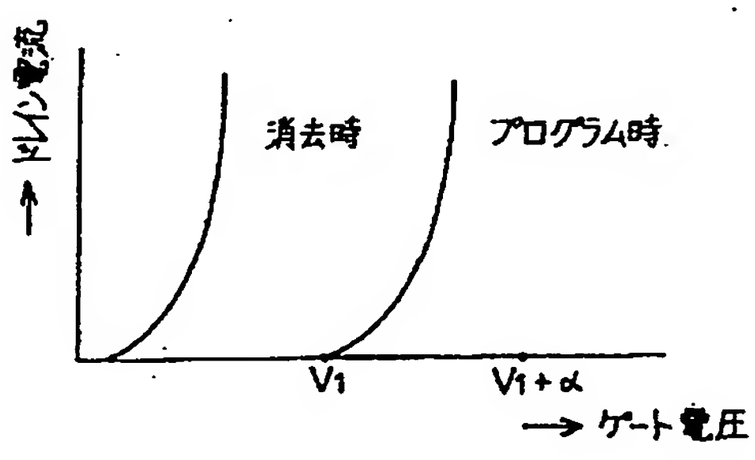
【符号の説明】

２	ＭＣＵチップ
３	入出力ポート
３１	ポート制御部
３２	ＣＰＵ
３３	モード制御部
４１	データバス
４２	アドレスバス
５１	主記憶部
５２	補助記憶部
５３	書き込み／読み出し（Ｒ／Ｗ）信号線
Ａ、Ｂ	トランジスタ
６１	電圧信号線
６２	バッファ
６３	行デコーダ
６４	列デコーダ
６５	センスアンプ
６６	書き込み／読み出し制御部

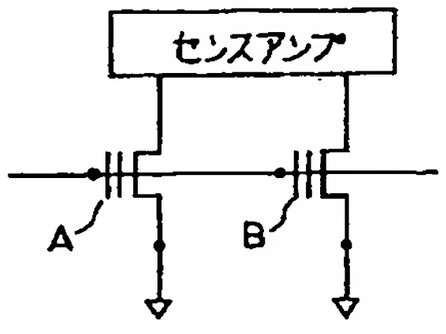
【図５】



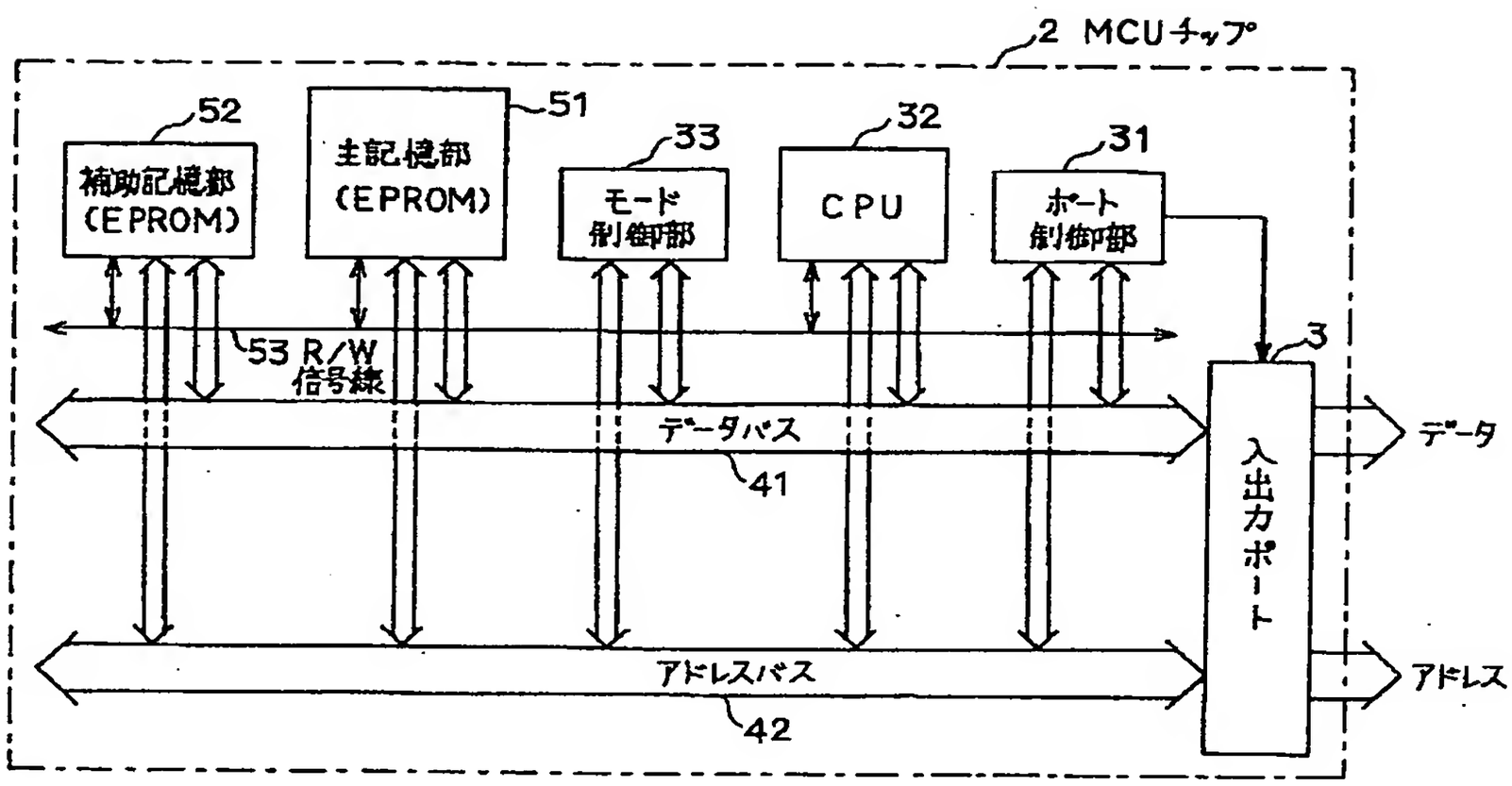
【図６】



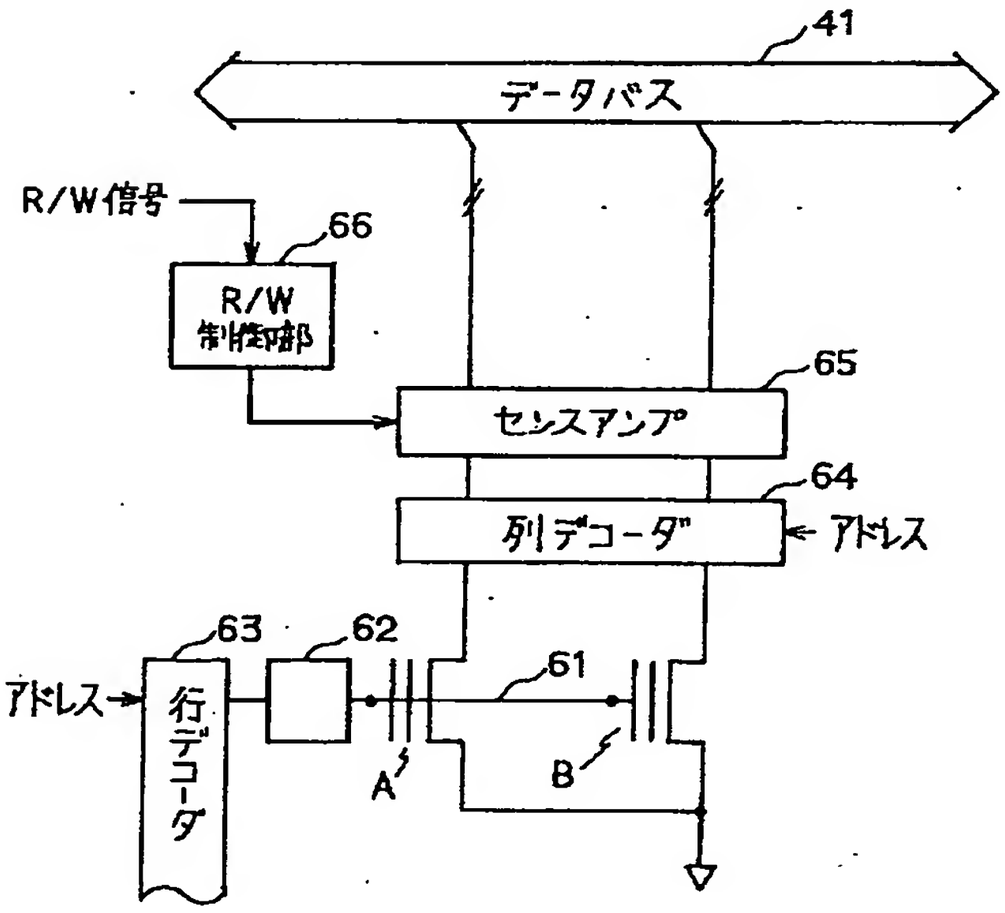
【図７】



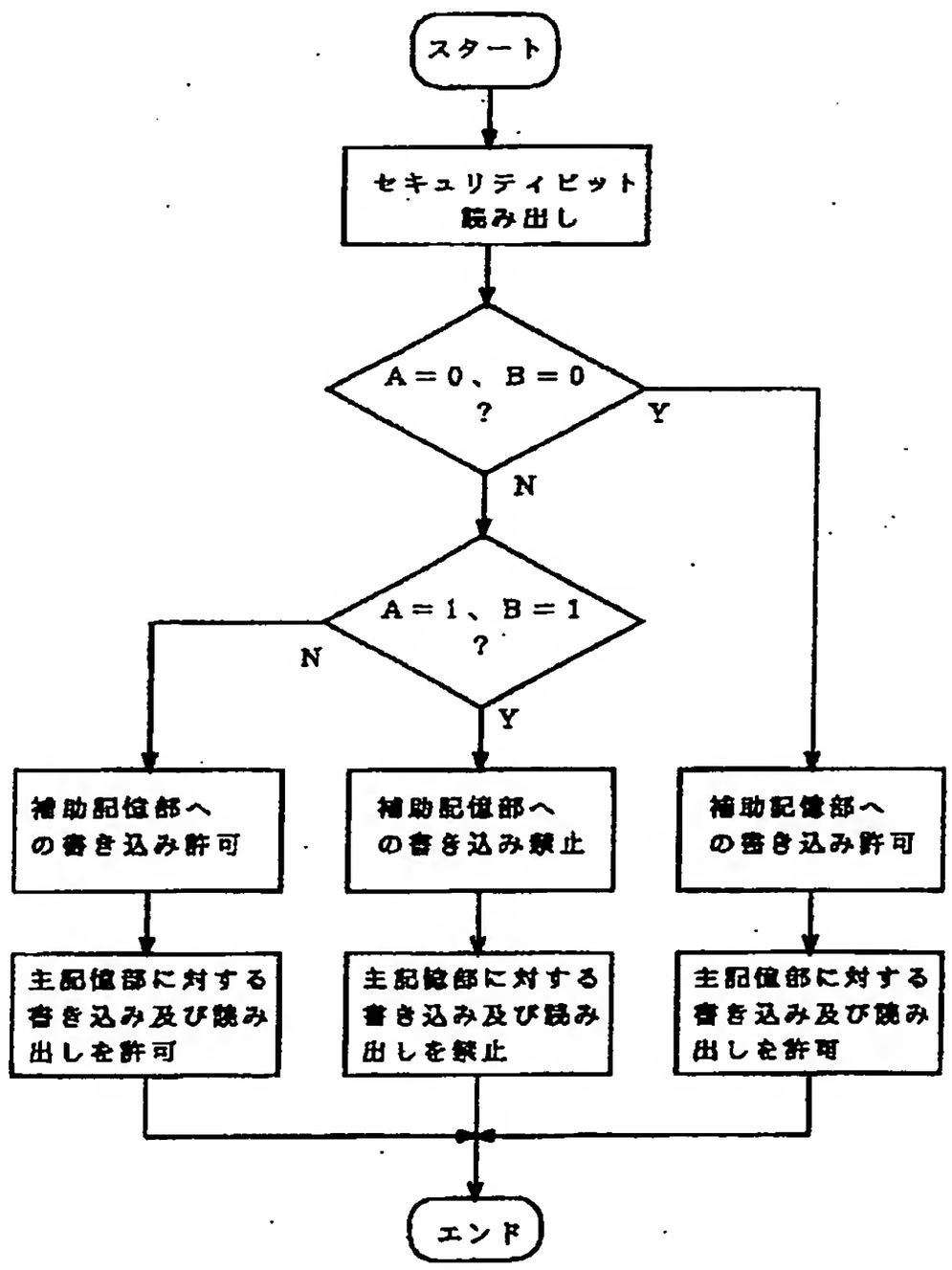
【図１】



【図２】



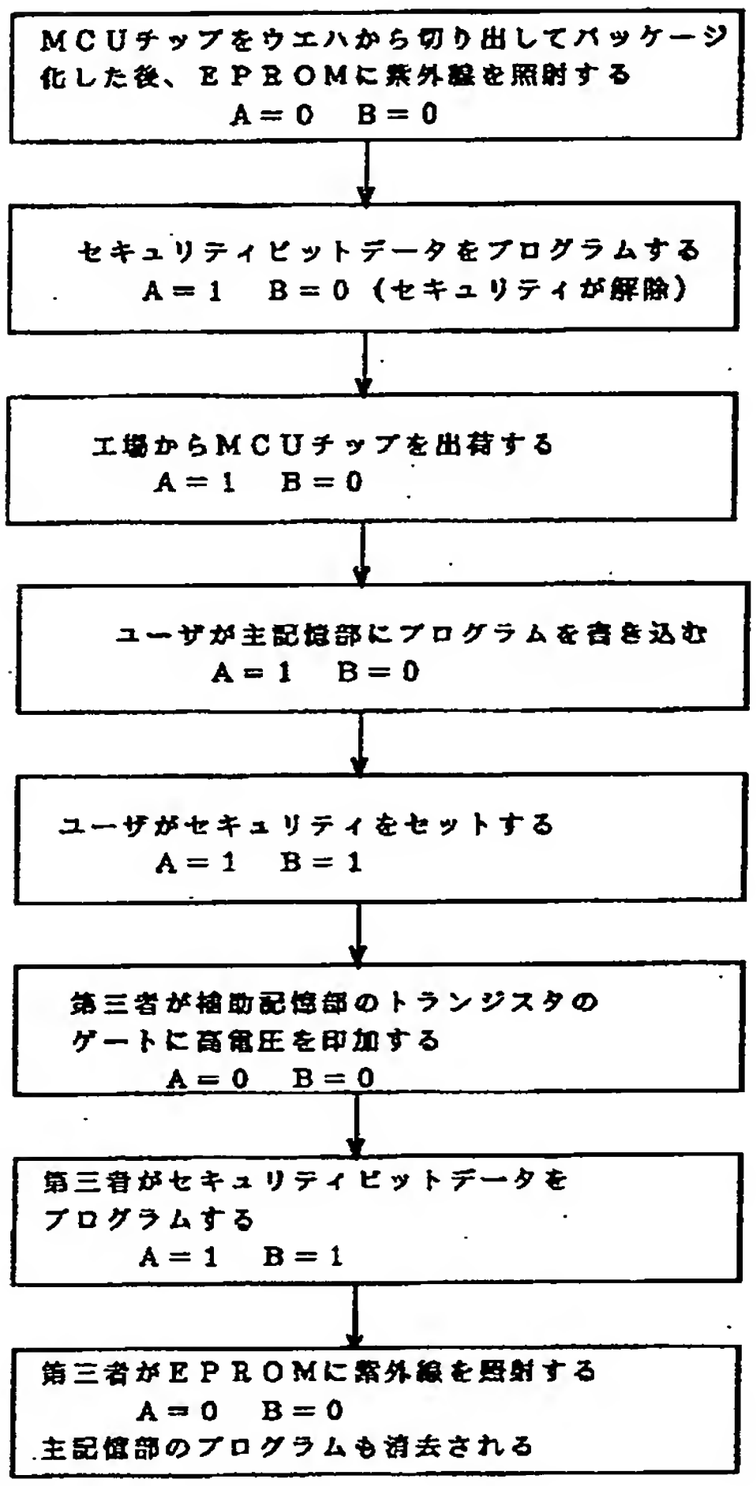
【図３】



【図８】

読み出し結果	処理状態	フローティングゲート
0	紫外線による消去	負電荷蓄積なし
1	プログラム	負電荷蓄積

【図４】



【図９】

読み出し結果		セキュリティの状態
A	B	
0	0	セット
0	1	解除
1	0	解除
1	1	セット